

ALSA Dev'n

United States District Court

FILED

WESTERN DISTRICT OF TEXAS

NOV 20 2007

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXASBY SV DEPUTY CLERK

UNITED STATES OF AMERICA

v.

STEVEN BRADLEY DAVIS, ()

CRIMINAL COMPLAINT

CASE NUMBER: A - 07 - M - 307

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about July through November 2007 in Travis County, in the Western District of Texas, and elsewhere, defendant(s) did, (Track Statutory Language of Offense)

During and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), knowingly transfer, possess, or use, without lawful authority, a means of identification of another person; Did knowingly and with intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices; Did intentionally access a computer without authorization and exceed authorized access, and did thereby obtain information contained in a financial record of a financial institution, or of a card issuer (as defined in 15 U.S.C. § 1602 (n)), or contained in a file of a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC 1681 et seq.); Did devise and intend to devise a scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, and to transmit or cause to be transmitted by wire communication in interstate or foreign commerce any writing, sign, signal, picture, or sound for the purpose of executing such scheme; Did knowingly execute and attempt to execute a scheme artifice to defraud a financial institution; or to obtain any of the money, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses; and Did conspire together and with each other to commit an offense against the United States, namely, one or more of the aforementioned offenses, and one or more Defendants did an act to effect the object of the conspiracy,

In violation of Title 18 United States Code, Section(s) 371, 1028A, 1029, 1030, 1343, and 1344

I further state that I am a(n) Special Agent, United States Secret Service and that this complaint is based on the following facts: Official Title

SEE ATTACHED AFFIDAVIT.

Continued on the attached sheet and made a part hereof.

X Yes CL No

Signature of Affiant

Sworn to before me, and subscribed in my presence

11/20/07

ANDREW W. AUSTIN
United States Magistrate Judge

Name and Title of Judicial Officer

at Austin, Texas

City and State

AW Austin
Signature of Judicial Officer

2. I respectfully submit this affidavit in support of the Government's application in support of a Criminal Complaint against Steven Bradley DAVIS, [REDACTED] and [REDACTED] of violations of Title 18 United States Code, Section 371 (Conspiracy to commit offense or to defraud United States), Section 1028A (Aggravated identity theft), Section 1029 (a) (3) (Fraud and related activity in connection with access device), Section 1030 (Fraud and related activity in connection with computers), Section 1343 (Fraud by wire, radio, or television) and Section 1344 (Bank fraud).

3. Title 18, United States Code Section 371 makes it a crime for two or more persons to conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and for any such persons to do any act to effect the object of the conspiracy.

4. Title 18, United States Code, Section 1028A makes it a crime for a person, during and in relation to any felony violation enumerated in 18 U.S.C. § 1028A(c), to knowingly transfer, possess, or use, without lawful authority, a means of identification of another person.

5. Title 18, United States Code, Section 1029(a)(3) makes it a crime for a person to knowingly and with intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices.

6. Title 18, United States Code, Section 1030 makes it a crime for a person to intentionally access a computer without authorization or exceed authorized access, and thereby obtain information contained in a financial record of a financial institution, or of a card issuer (as defined in 15 U.S.C. § 1602 (n)), or contained in a file of a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC 1681 et seq.).

7. Title 18, United States Code, Section 1343 makes it a crime for a person to devise or intend to devise any scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, and to transmit or cause to be transmitted by wire communication in interstate or foreign commerce any writing, sign, signal, picture, or sound for the purpose of executing such scheme.

8. Title 18, United States Code, Section 1344 makes it a crime for a person to knowingly execute, or attempt to execute, a scheme artifice to defraud a financial institution; or to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses.

Facts

9. In October 2007, FundsXpress and First Data Corporation reported an alleged theft of database information by STEVEN DAVIS, a former FundsXpress Database Administrator.

10. FundsXpress Financial Network Incorporated, a subsidiary of First Data Corporation, provides Internet Banking services to small to medium size banks and credit unions throughout the United States.

11. First Data Corporation provides electronic commerce and payment solutions for businesses worldwide. First Data serves over 5 million merchant locations, 1,900 card issuers and their customers. First Data Corporation products and services include merchant transaction processing; credit, debit, private-label, gift, payroll and other prepaid card offerings; fraud protection and authentication solutions; and electronic check acceptance services through TeleCheck. The company's STAR Network offers PIN-secured debit acceptance at 2 million

ATM and retail locations.

12. First Data Corporation, via TeleCheck (a check verification company owned by First Data Corporation) electronically verifies specific information presented during the negotiation of business and personal checks at retailers who subscribe to this service. When a check is presented as payment to a subscribing merchant, the check is electronically scanned by the cashier operating the register. Information obtained by the scanning of the check, is sent electronically (via wire) to Telecheck, who maintains a record of known "bad" checks in a computer database. Telecheck also verifies within that database that the bank routing number printed on the presented check is associated with a valid banking institution. Further, depending on the merchant's relationship with Telecheck, the merchant may also manually input the driver's license number of the person presenting the check and compare this number against a database of license numbers associated with known "bad" check writers.

13. DAVIS was employed at FundsXpress as one of the database administrators during 2001 and again from November 2002 until August 7, 2007, when his employment was suspended without pay for non-compliance with employment requirements. His responsibilities included maintaining the production database and keeping the data center functional. In this role, DAVIS had access to account information of client financial institutions. On August 7, 2007, DAVIS employment was terminated from FundsXpress.

14. On October 2, 2007, FundsXpress Customer Service department notified the FundsXpress Security Team of unauthorized checks written on customer accounts of the National Bank and Trust, La Grange, Texas. National Bank and Trust had several calls from customers who had noticed unauthorized purchases by check from Austin area Wal-Mart stores

on their National Bank and Trust accounts. The check numbers for the purchases were not within the range of the checks the customers were using, and in some cases the customers had never ordered checks. The support request by National Bank and Trust included information on three checking accounts used for five unauthorized purchases at Round Rock, Texas and Pflugerville, Texas Wal-Mart stores.

15. National Bank and Trust had noticed some unusual transactions on September 26 and 27, 2007. These unusual transactions involved account numbers and routing numbers appearing on checks that did not match the names on the checks. National Bank and Trust discovered all the effected customers were online banking enabled. Furthermore, the account numbers used on the checks had leading zeros (0s). These leading zeros (0s) are a characteristic of the FundsXpress interface with National Bank and Trust. The account numbers used on the fraudulent checks were padded with leading zeros (0s), which strongly indicates the origin of the account number. There had also been fraudulent transactions at Austin area Walgreens, HEB and Home Depot stores.

16. On or about October 4, 2007, National Bank and Trust indicated that it had received additional fraudulent checks. One of these checks was negotiated during a purchase of parts at BMW of Austin, and another was negotiated during a purchase at an Austin, TX area Wal-Mart. The check written to BMW of Austin, in the amount of \$261.72, was presented in the name of Steve Barnett, 3216 Willow Terrace, Kyle, Texas 78540. An invalid Texas driver's license number (XXXX6681)¹ was hand-written on the check as a means of identification. The

¹ To protect privacy and security concerns, only up to the last four digits of financial or business account numbers or personal identifiers referenced in this affidavit are included. See proposed Fed. R. Crim. P. 49.1(a)(4) (to be

routing number on the check is 113104534; the account number on the check is 0000XXXX56. Routing number 113104534 present on the check negotiated at BMW of Austin has been identified as the routing number for National Bank and Trust of La Grange, Texas.

17. Surveillance conducted during this investigation observed a gold BMW sedan, parked in DAVIS' driveway, bearing Texas license plate 641-CRH. Texas Department of Public Safety records indicate this vehicle is registered to DAVIS at 112 Mule Deer Court, Huno, Texas.

18. On October 5, 2007, a second bank, Spring Hill State Bank, of Longview, Texas, contacted FundsXpress to report suspicious transactions. Spring Hill State Bank reported activities nearly identical to the ones observed by National Bank and Trust. Fraudulent checks were being used at Austin area Walgreens, Wal-Mart and HEB. These fraudulent checks drawn on Spring Hill State Bank accounts were also created with account numbers containing leading zeros (0s).

19. On or about October 5, 2007, National Bank and Trust indicated that it had been in contact with Wal-Mart's asset protection department regarding the negotiation of counterfeit checks associated with this investigation. Surveillance video from Wal-Mart store #5479 located at 1548 FM 685, Pflugerville, Texas, showed one or more individuals who negotiated two fraudulent checks on September 27, 2007.

20. Information from BMW of Austin indicated that the parts purchased with the fraudulent check referenced in Paragraph 16 above were left and right window regulators and

effective December 1, 2007, absent contrary Congressional action). An "X" has been substituted in place of a digit for all but the last two to four digits. The full numbers are known to Your Affiant.

body molding. Notably, DAVIS drove a late model BMW whose driver and passenger windows were recently not functional. During the course of this investigation, it has been determined that the windows on DAVIS' BMW sedan are now functional, indicating that DAVIS may have been involved in the fraudulent purchase of the window regulators at BMW of Austin.

21. On or about October 5, 2007, Avery Buffington, Information Security Manager for FundsXpress, viewed the surveillance videos of September 27, 2007, and recognized DAVIS as the driver of a large, dark colored SUV with three passengers. Two of the individuals arriving with DAVIS are observed in the video passing fraudulent checks. Ms. Buffington reportedly recognized DAVIS in additional surveillance videos from various surveillance cameras during the same visit.

22. The Pflugerville Police Department was conducting a separate but related investigation involving a person who had purchased and attempted to return sewing machines at Wal-Mart utilizing a fraudulent check. Detective Chet Vronka of the Pflugerville Police Department identified this suspect as [REDACTED] and subsequently obtained a warrant for [REDACTED] arrest.

23. During his employment with FundsXpress, DAVIS was assigned two company owned computers at the FundsXpress office at 11950 Jollyville Road, Austin, Texas 78759. One computer was running Windows XP and the other was running Linux. DAVIS' Windows and Linux computer systems were imaged (i.e., the hard drives were duplicated) by Jim Clark, Lead Windows System Administrator with FundsXpress.

24. On October 11, 2007, Scott Janco, Manager, TeleCheck Information Security, forwarded the images of the Windows and Linux systems and DAVIS' hard drive from his Linux

computer to Richard Van Luvender, Director, First Data Corporation, InfoSec Incident Response, Wilmington, Delaware. Mr. Van Luvender has expertise in network and computer security information and intellectual property protection, and industry-specific regulatory requirements.

25. Forensic examination of DAVIS' computers conducted by Mr. Van Luvender on October 12, 2007, discovered email communications between DAVIS and his wife Kim DAVIS regarding the financial troubles they were experiencing. The financial troubles included but were not limited to, foreclosure on their house, missed car payments, various utilities being shutoff or threatened to be shutoff.

26. First Data Corporation was able to determine that DAVIS accessed the FundsXpress building, 11950 Jollyville Road, Austin, Texas, using his key access card on June 30, 2007, at approximately 11:49 PM; and that DAVIS' Linux and Windows systems were accessed using his unique user ID and password during the early morning of July 1, 2007.

27. Additional forensic examinations conducted by Mr. Van Luvender determined that, during the above mentioned logon on July 1, 2007, DAVIS extracted and copied numerous account numbers and routing numbers pertaining to several financial institutions from the production database files of FundsXpress. The forensic examination established that DAVIS used his Linux system to access data from the production database files and download them to a removable USB storage device.

28. Investigation by First Data revealed that shortly before July 1, 2007, DAVIS volunteered - without supervisor approval - to work on July 1, 2007. The work DAVIS volunteered for was a scheduled maintenance outage that two other employees were already scheduled to work. This gave DAVIS a reason to be at FundsXpress on the day he extracted and

copied the information from the production database files. The access and downloading of information from the FundsXpress database by DAVIS was not authorized nor within the scope of DAVIS' duties. Furthermore, DAVIS was not scheduled to work on the maintenance outage on July 1, 2007, and did not have any legitimate reason to extract and copy database files.

29. Analysis of surveillance video obtained from Wal-Mart store #5479 on September 27, 2007, along with analysis of associated transaction records, indicates that STEVEN BRADLEY DAVIS, [REDACTED] and [REDACTED] arrived at the Wal-Mart in a dark colored Chevrolet Suburban. Surveillance video shows [REDACTED] and [REDACTED] exiting the rear seat of the dark colored Chevrolet Suburban followed by DAVIS and [REDACTED] exiting the front seat of the Chevrolet Suburban and walking toward the entrance of the store. Surveillance video shows DAVIS is the driver of the Chevrolet Suburban.

30. Surveillance video from inside the store depicts [REDACTED] approaching a register and initiating a transaction. While at the register, he is joined by [REDACTED] for a brief moment. Video and transaction records obtained from Wal-Mart indicate [REDACTED] presented a fraudulent check bearing routing number 113104534, account number 0000XXXX52, for a purchase totaling \$396.47. Surveillance video from inside the store also depicts EVANS initiating a transaction at the same register. Video and transaction records obtained from Wal-Mart indicate EVANS presented a fraudulent check bearing routing number 113104534, account number 0000XXXX11, for a purchase totaling \$531.95. Surveillance video depicts DAVIS, [REDACTED] and [REDACTED] exiting the Wal-Mart store and departing in the same dark colored Chevrolet Suburban driven by DAVIS.

31. As previously described, routing number 113104534, present on the checks fraudulently negotiated by [REDACTED] and [REDACTED] on September 27, 2007 at Wal-Mart store # 5479, is the financial institution routing number for the National Bank and Trust of La Grange, Texas.

32. On November 7, 2007, surveillance was conducted at the residence of STEVEN DAVIS, 112 Mule Deer Court, Hurto, Texas. During this surveillance, [REDACTED] was observed departing DAVIS' residence driving a red Kia Sportage bearing Texas license plate S17-PYC. A registration check of the vehicle indicated the vehicle was registered to Lawrence Motors DBA #1 Affordable Auto Sales, 8301 Research Blvd., Austin, Texas. [REDACTED] was known to the agents conducting the surveillance to have a valid state jail felony warrant issued by the Pflugerville Police for theft. Additionally, [REDACTED] had been identified by Detective Vronka as using a fraudulent check drawn on one of the bank accounts that were extracted and copied by DAVIS from FundsXpress.

33. On November 7, 2007, [REDACTED] was arrested on the outstanding Pflugerville PD warrant. A search incident to arrest of [REDACTED] Kia Sportage vehicle revealed a white plastic Wal-Mart bag located in the rear compartment of the vehicle. In the white plastic Wal-Mart bag, there was a receipt for the purchase of a desktop computer. The receipt indicated the purchase was paid for by a check. Additionally, the receipt indicated the return of the desktop computer at an undetermined Wal-Mart. Further investigation indicated the check written for the personal computer was drawn on one of the accounts that was downloaded and copied by DAVIS.

34. On November 15, 2007, agents learned that Room 191 of the Travel Lodge, 6200

Middle Fiskville, Austin, Texas, was registered to Steve Davis with an address of 112 Mule Deer Court, Hunto, Texas 78634.

35. On November 16, 2007, surveillance at the Travel Lodge observed DAVIS driving a 1997 Chevrolet Suburban, bearing Texas license plate 757-DCN. DAVIS was observed seated in the driver's side back seat of the Suburban working on a laptop computer. Later that same day, DAVIS was observed leaving the hotel, then returning to the hotel and entering Room 191.

36. On November 17, 2007, agents learned that Travel Lodge Room 191 had been vacated and that items had been abandoned in the room. Among the items found in the room were fraudulent Texas driver's licenses which appear to have been manufactured utilizing personal computer programs and technology. Also among the items in the room were apparently genuine Bank of America personal checks bearing the names of "Dennis Wooster" and "Melanie Wooster".

37. On or about November 17, 2007, the Round Rock Police Department (RRPD) arrested [REDACTED] and Christina Hamby. According to RRPD, [REDACTED] and Hamby were contacted during a routine traffic stop on this date. During the course of this traffic stop, Hamby, the driver of the vehicle, gave RRPD permission to search the car. During the search, RRPD found several counterfeit Texas driver's licenses bearing various names and photographs of TAYLOR's likeness. RRPD also found several counterfeit checks bearing names which matched some of the counterfeit Texas driver's licenses. A laptop computer was also seized, along with a computer disk for a commercially available check-writing program known as "Versachek." Also seized were several identification-style photographs of [REDACTED] along

with one or more counterfeit driver's licenses bearing this photograph of [REDACTED] and bearing various names other than his own.

38. RRPD also seized a label maker. Inspection of the label maker revealed a label on the underside of the label maker bearing the name "Crucial Walker." On or about October 24, 2007, officers conducted a surreptitious search of the garbage can outside of DAVIS's residence in Hutto, Texas. During this search, a recent cellular telephone bill bearing the name "Crucial Walker" was discovered.

39. On or about November 19, 2007, surveillance observed DAVIS driving a dark blue Chevrolet Suburban registered in his name, which also contained at least three other

40. After DAVIS departed, the HEB cashier who handled this transaction was briefly interviewed. According to the cashier, the check and the individual attempting to pass the check "did not seem right," which is why the cashier attempted to call the store manager. The cashier also stated that the last name of the account holder appearing on the check was "Wooster." Further efforts that day to surveil DAVIS' Suburban were unsuccessful.

41. On November 20, 2007, DAVIS' BMW vehicle was observed in the driveway of his residence; however, DAVIS' Chevrolet Suburban was not present. The Suburban was later located parked at the Dell Diamond baseball park in Round Rock, Texas, where DAVIS' wife, Kimberly Davis, is employed by the Round Rock Express baseball team. It appears DAVIS returned to his residence sometime after surveillance was discontinued in the early hours of November 20, 2007.

42. As of November 14, 2007, there has been an estimated loss of over \$45,000.00 from approved transactions and over \$22,000.00 in declined transactions attributed to accounts for which DAVIS obtained information without authorization from the FundsXpress database. There have been approximately 8 financial institutions and 79 accounts that have shown fraudulent activity as of this time.

Conclusion

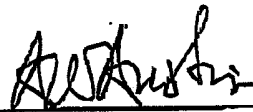
43. Based on the foregoing facts, there is probable cause to believe that Steven Bradley DAVIS, [REDACTED] and [REDACTED] did commit and attempt to commit one or more offenses in violation of Title 18, United States Code, Sections 1028A, 1029, 1030, 1343, and 1344, and did conspire to commit one or more of said offenses, in violation of Title 18, United States Code, Section 371.

FURTHER AFFIANT SAYETH NAUGHT.



NGUYEN C VU
Special Agent
United States Secret Service
Austin, Texas

Subscribed and sworn to before me at Austin, Texas, on this 20th day of November,
2007.



UNITED STATES MAGISTRATE JUDGE